Anlage zum Vertrag zur Datenverarbeitung im Auftrag vom TT.MM.20JJ

**Technische und organisatorische Maßnahmen für die Fernwartung**

Datum

Die verantwortliche Stelle hat technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften des einschlägigen Datenschutzgesetzes entsprechende Datenverarbeitung zu gewährleisten. Die Maßnahmen haben insbesondere das Ziel, die Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit und Resilienz sicherzustellen. Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen, die bei einer Fernwartung getroffen werden.

1. **Sicherstellung der Vertraulichkeit**
	1. **Zugangskontrolle**
		1. **Verantwortlicher**

Die Tätigkeiten, die durch den Auftragsverarbeiter bei den Fernwartungsarbeiten und/oder Live-Support durchgeführt werden, sind durch den Verantwortlichen kontrollierbar *(einer von beiden Punkten muss erfüllt sein)*:

[ ]  Die Tätigkeit des Auftragsverarbeiters kann an einem Kontrollbildschirm in Echtzeit verfolgt werden (Live-Support[[1]](#footnote-1)).

Grundsätzlich werden beim Live-Support notwendige Passwörter durch den Verantwortlichen eingegeben, der die Arbeiten am Kontrollbildschirm verfolgt.

[ ]  Es erfolgt eine Kontrolle über die Protokollierung am System. Hierzu konfiguriert der Verantwortliche eine automatische Protokollierung der Fernwartungsarbeiten[[2]](#footnote-2). Nach Abschluss der Arbeiten werden die Protokolle überprüft und zu Kontrollzwecken für ein Jahr[[3]](#footnote-3) aufbewahrt. Dies ist wie folgt realisiert:

**Erläuterung:**

Bitte beschreiben Sie, wie die Protokollierung und die Aufbewahrung (Ort, Medium, Art der Aufbewahrung) erfolgen. Aus der Beschreibung muss sich ergeben, dass die Protokollierung so detailliert ist, dass damit die durchgeführten Tätigkeiten eindeutig identifizierbar sind.

[ ]  **Der Auftragsverarbeiter muss darüber hinaus zu seiner Aufgabenerfüllung zwingend Passwörter erhalten.**

Für die Durchführung der Arbeiten ist es im vorliegenden Fall zwingend erforderlich, dem Auftragsverarbeiter für die Fernwartungsarbeiten und/oder den Live-Support zusätzliche Passwörter zu geben. Der Verantwortliche ändert diese unverzüglich nach Beendigung der Fernwartungsarbeiten und/oder des Live-Supports. Sofern die Konten speziell für die Fernwartung eingerichtet sind, reicht es diese Zugänge zu sperren. Dies muss in der gesamten Authentifizierungskette erfolgen (Firewall-Regeln, VPN-Zugang, Benutzerkonten usw. siehe auch 2.2.1 und 2.3.1).

**Erläuterung:**

Hier bitte Ausführungen zu organisatorischen Regelung zur Änderung der Passwörter, sofern diese nicht direkt und unverzüglich durch den Benutzer selbst geändert werden kann, oder zur Sperrung der Authentifizierungskette.

Der Verantwortliche stellt durch entsprechende Infrastruktur (Hardware/Software) und einer dementsprechend sicheren Konfiguration und Rechtevergabe sicher, dass durch den Zugriff für die Fernwartungsarbeiten und/oder den Live-Support nur auf die Rechner, Netzwerkabschnitte und Ressourcen zugegriffen werden kann, die für die Aktivität der Fernwartung und/oder den Live-Support zwingend erforderlich ist.

* + 1. **Auftragsverarbeiter**

Die für die Fernwartungsarbeiten und/oder den Live-Support verwendeten Rechner sind im Eigentum des Auftragsverarbeiters und sind nur für den rein dienstlichen Gebrauch zugelassen. Es ist ausschließlich Software für den dienstlichen Gebrauch installiert. Eine private Nutzung ist explizit ausgeschlossen.

Das Betriebssystem auf den Rechnern, die für die Fernwartungsarbeiten und/oder den Live-Support genutzt werden, verfügt über eine Benutzerverwaltung so, dass mittels eines Rollen- und Rechtekonzepts die Zugriffsmöglichkeiten eingeschränkt sind und ohne gültige Authentifizierung verhindert werden. Die Rechte werden restriktiv vergeben. Es gibt eine klare und technisch erzwungene Trennung der Rollen und Rechte für administrative Tätigkeiten und für die Tätigkeiten der Fernwartung. Insbesondere sind administrative Rechte für Tätigkeiten bei der Fernwartung auf den Rechnern ausgeschlossen. Die Zugriffsmöglichkeiten können nach Daten, Programmen und Art des Zugriffs differenziert werden und sind für die Erforderlichkeit der Fernwartungsarbeiten entsprechend eingerichtet.

Die Rechteverwaltung der Datenträger ist abgestuft auf der Ebene der Laufwerke, Verzeichnisse, Unterverzeichnisse, Dateien und Freigaben. Dabei sind die Rechte restriktiv vergeben.

Das Betriebssystem ist auf dem aktuellen Stand der Technik. Verfügbare Sicherheitsaktualisierungen für das Betriebssystem und der installierten Software werden regelmäßig durchgeführt. Mindestens alle 14 Tage erfolgt eine Prüfung auf eine Verfügbarkeit von Sicherheitsaktualisierungen sowie deren unverzügliche Installation.

Die Rechner verfügen über eine aktuelle Sicherheitssoftware (Antiviren-Software). Die Aktualisierung dieser Software sollte täglich geprüft und ggfs. installiert werden. Keinesfalls wird die Aktualisierung über mehr als 7 Tage ausgesetzt. Es ist durch Systemrechte sichergestellt, dass nur administrative Benutzer die Sicherheitssoftware konfigurieren und aktivieren oder deaktivieren können.

Die Datenträger werden regelmäßig (mind. einmal im Monat) mit der Sicherheitssoftware auf schädliche Software überprüft. Sollte eine Infizierung festgestellt werden, so wird dieses Gerät erst dann wieder in Betrieb genommen, wenn zweifelsfrei festgestellt wurde, dass der oder die Schädlinge vollständig entfernt wurden. Ggfs. wird eine Neuinstallation des Systems vorgenommen.

Sollte das Gerät vor der Entdeckung einer Schadsoftware bereits für Fernwartungsarbeiten und/oder Live-Support beim Verantwortlichen eingesetzt worden sein, so wird diesem der Vorfall unverzüglich angezeigt.

Das System wird bei einer Inaktivität von mehr als 5 Minuten automatisch gesperrt und kann nur durch Eingabe des gültigen Passwortes wieder entsperrt werden.

Alle Tätigkeiten für die Fernwartungsarbeiten und/oder den Live-Support erfolgen ausschließlich aus dem Firmennetz des Auftragsverarbeiters heraus.

**Folgende Software ist installiert (Erläuterung):**

Eingesetzte(s) Betriebssystem(e) und Version(en)

Antivirensoftware und Version(en)

* 1. **Zutrittskontrolle**
		1. **Verantwortlicher**

Die Verbindung für Fernwartungsarbeiten und/oder Live-Support ist so gestaltet, dass diese jederzeit durch den Verantwortlichen unterbrochen werden kann.

Nach Abschluss der Fernwartungsarbeiten und/oder des Live-Supports stellt der Verantwortliche sicher, dass die Verbindung wieder abgebaut ist.

**Erläuterung:**

Bitte Erläuterung einfügen, wie technisch und organisatorisch sichergestellt wird, dass die Verbindung zur Fernwartung unterbrochen werden kann und nach Abschluss der Arbeiten abgebaut ist. Z.B. "Dies wird dadurch erreicht, dass..."

* + 1. **Auftragsverarbeiter**

Die stationären Arbeitsplatzrechner, die für die Fernwartungsarbeiten und/oder Live-Support genutzt werden, stehen in einem nicht öffentlich zugänglichen Büroraum. Bei längerer Abwesenheit, zum Beispiel für Termine oder nach Arbeitsende, ist der Raum verschlossen. Die Schlüsselvergabe unterliegt einer klaren Regelung, so dass der Personenkreis, der Zutritt zu den Büroräumen hat, zu jeder Zeit klar und eindeutig identifizierbar und benennbar ist.

**Erläuterung:**

Verweis auf die Dienstanweisung/Dokumentation des Auftragsverarbeiters o.ä. zur Vergabe der Schlüssel bzw. Zutrittsberechtigung zu den Räumen.

* 1. **Pseudonymisierung**
		1. **Verantwortlicher**

Sofern es für die Bearbeitung eines Support-Falls erforderlich ist, personenbezogene Daten beim Auftragsverarbeiter zu speichern, so ist vor jeder Übertragung an den Auftragsverarbeiter durch den Verantwortlichen zu prüfen, ob für die Bearbeitung nicht pseudonymisierte oder anonymisierte Echtdaten oder Testdaten ausreichen. Dies kann in Rücksprache mit dem Auftragsverarbeiter erfolgen.

Bei der Pseudonymisierung muss darauf geachtet werden, dass die Daten derart transformiert werden, dass auch durch die Kombination der einzelnen Merkmale und das Hinzuziehen von weiteren Quellen für den Auftragsverarbeiter kein Personenbezug herstellbar ist. Weitere Quellen sind in diesem Zusammenhang öffentlich zugängliche Quellen, insbesondere Daten, die zum Beispiel auf dem Webauftritt des Verantwortlichen oder in anderen öffentlich zugänglichen Datenbeständen publiziert sind.

* + 1. **Auftragsverarbeiter**

Sofern für die Aufgabenerfüllung – sei es als Ausnahme oder als Regelfall - die Übertragung von personenbezogenen Daten des Verantwortlichen an den Auftragsverarbeiter zwingend erforderlich ist, müssen die Punkte 2.2.1 mit Option 1 und Punkt 2.3.2 mit Option 1 gewählt sein.

* 1. **Verschlüsselung**
		1. **Auftragsverarbeiter**

[ ]  **Mobile Rechner oder Geräte**

Die Datenträger in den mobilen Rechnern, sofern diese für Fernwartungsarbeiten und/oder Live-Support eingesetzt werden, sind mit anerkannt starken kryptografischen Algorithmen, Verfahren und Software nach dem Stand der Technik vollständig verschlüsselt und mit einem Passwort gesichert (siehe hierzu die Passwortrichtlinie und für die Mindestanforderungen Punkt 2.2).

**Die Verschlüsselung ist wie folgt realisiert (Erläuterung):**

Software zur Datenträgerverschlüsselung, Version(en) und Konfiguration(en):

1. **Sicherstellung der Integrität**
	1. **Übertragungskontrolle**

Der Verantwortliche und der Auftragsverarbeiter stellen durch eine kryptografisch starke Verschlüsselung nach dem Stand der Technik sicher (siehe 2.2), dass keine personenbezogenen Daten im Rahmen der Fernwartungsarbeiten und/oder des Live-Supports an einen fremden Dritten übermittelt werden.

* 1. **Verschlüsselung**

Die Verbindung, die zum Zweck der Fernwartungsarbeiten und/oder des Live-Supports zu den Systemen des Verantwortlichen aufgebaut wird (Online-Verbindung), hat eine kryptografisch starke Verschlüsselung nach dem Stand der Technik.

Derzeit bedeutet dies mindestens

* AES mit mindestens 128 Bit Schlüssellänge als Blockchiffre,
* SHA2 als Hash-Algorithmus,
* RSA mit einem mindestens 2048 Bit langen Schlüssel,
* TLS in aktuell als sicher anerkannter Version als Protokoll oder ein anerkannt äquivalent sicheres.

Die Verschlüsselung von personenbezogenen Daten auf mobilen Datenträgern, in Containern (z. B. verschlüsselte Dateien, Archive, E-Mail o.ä.) oder die Verschlüsselung von Datenträger in mobilen Rechnern genügt mindestens folgenden derzeitigen Anforderungen:

* AES mit mindestens 128 Bit Schlüssellänge als Blockchiffre,
* SHA2 als Hash-Algorithmus,
* einem Passwort entsprechend der Richtlinie für verschlüsselte Datenträger oder einem RSA Schlüsselpaar mit mindestens 2048 Bit. Der private Schlüssel ist dabei mit einem Passwort entsprechend der Passwortrichtlinie für verschlüsselte Datenträger (siehe Passwortrichtlinie) gesichert.
	+ 1. **Verantwortlicher**

Der Verantwortliche stellt einen geeigneten Zugang zur Verfügung, der kryptografisch stark nach dem Stand der Technik verschlüsselt ist und sowohl die Authentizität der Kommunikationspartner als auch die Integrität der Verbindungsdaten sicherstellt.

Dies gilt sowohl für Online-Verbindungen als auch für den Transport personenbezogener Daten mit mobilen Datenträgern oder Containern.

**Der Zugang ist wie folgt technisch realisiert (Erläuterung):**

Erläuterung, wie der Zugang technisch realisiert ist.

[ ]  **Transport von personenbezogenen Daten an den Auftragsverarbeiter ist außerhalb der Online-Verbindung erforderlich.**

Es ist zwingend erforderlich, dass personenbezogene Daten im Rahmen der Fernwartungsarbeiten und/oder des Live-Supports an den Auftragsverarbeiter außerhalb der Online-Verbindung versendet werden. Die personenbezogenen Daten werden vom Verantwortlichen kryptografisch stark nach dem Stand der Technik verschlüsselt, bevor diese an den Auftragsverarbeiter versendet werden (für die Mindestanforderungen siehe 2.2).

Bei dem Versand mit einem Datenträger oder Container genügt das Passwort der Passwortrichtlinie für verschlüsselte Datenträger (siehe Passwortrichtlinie) und wird auf einem anderen Weg zum Auftragsverarbeiter versandt als die verschlüsselten Daten selbst.

**Erläuterung:**

Bitte beschreiben Sie hier, wie verschlüsselt wird. Entweder erfolgt dies durch eine Transportverschlüsselung oder durch einen verschlüsselten Datenträger oder Container.

**[ ]  Transport von personenbezogenen Daten bei einer Online-Verbindung für den Live-Support:**

Der Verantwortliche gestattet nur Zugriff mit einer Live-Support-Software auf die zu unterstützenden Systeme, die eine kryptografisch stark verschlüsselte Punkt-zu-Punkt-Verbindung nach dem Stand der Technik ermöglicht und die die genannten Mindestvoraussetzungen für eine Online-Verbindung erfüllt (siehe 2.2).

* + 1. **Auftragsverarbeiter**

Sollte die Tätigkeit zur Fernwartung und/oder zum Live-Support nicht unmittelbar aus dem Firmennetz des Auftragsverarbeiters heraus erfolgen, so ist zuerst eine VPN-Verbindung oder eine äquivalent sichere Verbindung in das Firmennetz des Auftragsverarbeiters aufzubauen.

Die Verbindung für Fernwartungsarbeiten und/oder Live-Support erfolgt ausschließlich kryptografisch stark nach dem Stand der Technik verschlüsselt von Punkt zu Punkt, so dass zwischen dem Rechner des Auftragsverarbeiters, auf dem die Fernwartungsarbeiten und/oder der Live-Support erfolgen, und dem Endpunkt beim Verantwortlichen keine Komponente liegt, die den Datenstrom im Klartext einsehen oder manipulieren kann.

Die Personen, die die Fernwartungstätigkeit und/oder den Live-Support durchführen, sind dem Verantwortlichen auf dessen Anforderung namentlich zu nennen.

[ ]  **Fernwartungsarbeiten und/oder Live-Support erfolgen über statische IP-Adressen:**

Die IP-Adresse(n) oder das IP-Netz, aus dem heraus die Fernwartungsarbeiten und/oder Live-Support erfolgt, ist/sind folgende: IP-Adresse(n) oder das IP-Netz, aus dem die Fernwartung erfolgt

Der Zugriff auf die zu wartenden Systeme ist durch den Verantwortlichen auf die oben genannten IP-Adressen durch technische Maßnahmen, z.B. an der Firewall, beschränkt.

[ ]  **Fernwartungsarbeiten und/oder Live-Support erfolgen über dynamische IP-Adressen.**

* 1. **Eingabekontrolle**
		1. **Verantwortlicher**

[ ]  **Fernwartungsarbeiten:**

Der Verantwortliche konfiguriert die Systeme, auf die im Rahmen der Fernwartungsarbeiten zugegriffen werden so, dass nur auf die Programme, Dateien, Verzeichnisse und Daten zugegriffen werden kann, die für die Tätigkeit der Fernwartung zwingend erforderlich sind. Dabei werden die vergebenen Rechte auf der Ebene des Betriebssystems, der Serverdienste und der Anwendung berücksichtigt.

[ ]  **Live-Support:**

Der Verantwortliche hat nur die Programme geöffnet, die zur Behebung des Problems zwingend erforderlich sind. Er verfolgt die Tätigkeiten des Auftragsverarbeiters am Kontrollbildschirm und wird ggf. die Verbindung unterbrechen.

Grundsätzlich wird der Zugriff auf personenbezogene Daten durch den Verantwortlichen verhindert, sofern dies nicht zur Aufgabenerfüllung erforderlich ist.

[ ]  **Fernwartungsarbeiten:**

Die Tätigkeit der Fernwartung erfolgt über ein hierfür angelegtes Benutzerkonto, das durch den Verantwortlichen eingerichtet ist und nur über die für die Tätigkeit der Fernwartung zwingend notwendigen Rechte verfügt. Dieses Benutzerkonto verfügt grundsätzlich über keine Systemverwalterprivilegien.

Für Anwendungsprogramme, die über eine Benutzerverwaltung verfügen, gilt dies entsprechend.

Die Benutzerauthentifizierung wird durch das System und ggfs. durch die Anwendung mit Benutzername und Passwort erzwungen (siehe Passwortrichtlinie).

[ ]  **Live-Support:**

Während der Unterstützungsleistung des Auftragsverarbeiters ist der Verantwortliche zu jeder Zeit anwesend und beobachtet die Tätigkeiten des Auftragsverarbeiters. Insbesondere werden in dieser Zeit keine anderen Tätigkeiten vom Verantwortlichen wahrgenommen.

Der Zugriff des Auftragsverarbeiters auf das System des Verantwortlichen erfolgt nur nach persönlicher anlassbezogener Einwilligung des Verantwortlichen.

Der Kontrollbildschirm in Punkt 1.1.1 ist hier zwingende Voraussetzung.

[ ]  **Rechner für die Fernwartung:**

Für die Fernwartungsarbeiten ist es erforderlich, dass der Verantwortliche einen Arbeitsplatzrechner bei sich einrichtet[[4]](#footnote-4), auf den der Auftragsverarbeiter von extern zugreift. Auf diesem Arbeitsplatzrechner ist nur die zwingend erforderliche Software installiert.

* + 1. **Auftragsverarbeiter**

Rechner, die einen Netzanschluss haben, der direkten Zugang zu einem öffentlichen Netz hat (Internet, Firmennetz o. ä.), d.h. ohne vorgeschaltete Firewall betrieben werden, verfügen selbst über eine eigene Firewall. Dies gilt zwingend für mobile Rechner.

Die Firewall, vorgeschaltet oder auf dem Rechner selbst, ist so konfiguriert, dass nur das freigeschaltet ist, was explizit erlaubt ist, und dass Verbindungen nur erlaubt sind, die vom Rechner selbst initiiert werden.

Es ist durch Systemrechte sichergestellt, dass bei einer Firewall auf dem Rechner selbst nur administrative Benutzer diese konfigurieren und aktivieren oder deaktivieren können.

Auf dem Rechner des Auftragsverarbeiters für die Fernwartungsarbeiten und/oder den Live-Support werden grundsätzlich keine personenbezogenen Daten des Verantwortlichen gespeichert. Sollte dies zur Erfüllung der Tätigkeit zwingend erforderlich sein, werden folgende Bedingungen erfüllt:

* Nach Beendigung der Fernwartungsarbeiten und/oder des Live-Supports werden alle personenbezogenen Daten, die im Rahmen der Tätigkeit verarbeitet und gespeichert wurden, unverzüglich datenschutzgerecht gelöscht oder dem Verantwortlichen datenschutzgerecht übergeben.
* Sollten Ausdrucke angefertigt worden sein, so werden diese unverzüglich nach Beendigung der Tätigkeit datenschutzgerecht vernichtet. Ferner wird durch den Auftragsverarbeiter zumindest durch dienstliche Anweisungen ausgeschlossen, dass Kopien der Ausdrucke bei weiteren Systemen (Druckserver, Multifunktionsgerät o. ä.) angefertigt und gespeichert wurden. Sollte dies der Fall sein, so werden auch diese Kopien unverzüglich datenschutzgerecht gelöscht oder dem Verantwortlichen datenschutzgerecht übergeben.

[ ]  **Speicherung personenbezogener Daten beim Auftragsverarbeiter ist über Online-Verbindung hinaus erforderlich**

Im Rahmen der Fernwartungsarbeiten und/oder des Live-Supports kann es zwingend erforderlich sein, dass personenbezogene Daten über den Zeitraum der Online-Verbindung hinaus beim Auftragsverarbeiter gespeichert werden müssen. Diese Daten werden in einem stark kryptografisch gesicherten Container nach dem Stand der Technik (für die Mindestanforderungen siehe 2.2) oder gleichwertig gespeichert. Die Daten werden unverzüglich datenschutzgerecht gelöscht oder dem Verantwortlichen datenschutzgerecht übergeben, sobald diese für die Bearbeitung nicht mehr erforderlich sind. Die Dauer der Speicherung und Löschung ist dem Verantwortlichen anzuzeigen.

Das Betriebssystem, das auf den Rechnern für Fernwartungsarbeiten und/oder für Live-Support installiert ist, erzwingt eine Benutzerauthentifizierung mit Benutzername und Passwort (siehe Passwortrichtlinie).

[ ]  **Fernwartungsarbeiten:**

Alle Tätigkeiten, die im Rahmen der Fernwartungsarbeiten vorgenommen werden, werden durch den Auftragsverarbeiter schlüssig und nachvollziehbar dokumentiert, so dass zu jeder Zeit der zeitliche und inhaltliche Umfang der Tätigkeit als auch der Auftrag, der die Tätigkeit auslöst, als auch die beteiligten Personen benennbar sind.

[ ]  **Live-Support:**

Für die Tätigkeit des Live-Supports werden durch den Auftragsverarbeiter der Zeitpunkt, der Auftrag und die beteiligten Personen schlüssig und nachvollziehbar dokumentiert.

* 1. **Installation von Software**
		1. **Auftragsverarbeiter**

[ ]  Im Rahmen der Tätigkeit der Fernwartung und/oder des Live-Supports ist es zwingend erforderlich, dass durch den Auftragsverarbeiter Software installiert oder aktualisiert wird. Für diese Software stellt der Auftragsverarbeiter sicher, dass diese aus vertrauenswürdigen Quellen stammt und nach besten Wissen auf die Freiheit von schädlichen Code geprüft wurde. Dies betrifft sowohl die Software, die von Dritten bezogen und genutzt wird, als auch die Software, die ggfs. von Auftragsverarbeiter selbst entwickelt wird.

1. **Sicherstellung der Verfügbarkeit, Belastbarkeit und Resilienz**
	1. **Auftragsverarbeiter**

[ ]  **Zugangsdaten:**

Für die Fernwartungsarbeiten und/oder den Live-Support an den Systemen des Verantwortlichen werden Zertifikate, SSH-Schlüssel oder ähnliche Zugangsdaten für Systeme des Verantwortlichen durch den Auftragsverarbeiter verwendet. Diese sind gesondert gesichert aufbewahrt. Dabei wird ein kryptografisch stark verschlüsselter Container nach dem Stand der Technik (für die Mindestanforderungen siehe 2.2 und die Passwortrichtlinie) oder eine gleichwertige Sicherung verwendet.

Der Auftragsverarbeiter stellt durch interne Regelungen sicher, dass der Zugriff auf die Zugangsdaten auch durch einen benannten Stellvertreter möglich ist, sollte ein Vertretungsfall eintreten.

Es ist zu jeder Zeit technisch und/oder organisatorisch nachvollziehbar, auf welchen Medien die Zugangsdaten für die Fernwartung gespeichert sind, wie diese gesichert sind und von wem diese genutzt werden.

1. **Regelmäßige Überprüfung, Bewertung und Evaluierung der TOM**

In Bezug auf die Fernwartungstätigkeit und/oder den Live-Support ist ein Vertrag zur Auftragsdatenverarbeitung entsprechend dem einschlägigen Datenschutzgesetz zwischen dem Verantwortlichen und dem Auftragsverarbeiter abzuschließen[[5]](#footnote-5).

* 1. **Verantwortlicher**

Der Verantwortliche prüft regelmäßig, ob die von ihm zu treffenden technischen und organisatorischen Maßnahmen umgesetzt und eingehalten werden.

* 1. **Auftragsverarbeiter**

Der Auftragsverarbeiter prüft regelmäßig selbständig, ob die von ihm zu treffenden technischen und organisatorischen Maßnahmen umgesetzt und eingehalten werden.

Der Auftragsverarbeiter gewährleistet, dass er die zur Verarbeitung der personenbezogenen Daten des Verantwortlichen befugten Personen zur Vertraulichkeit und Verschwiegenheit verpflichtet hat und es ihnen untersagt ist, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Unabhängig von einer gesetzlichen Verpflichtung informiert er sie regelmäßig über das Datengeheimnis und Dienstanweisungen zum Datenschutz.

Der Auftragsverarbeiter trifft Regelungen zur Löschung oder Vernichtung personenbezogener Daten, die bei den Fernwartungsarbeiten und/oder dem Live-Support gespeichert oder gedruckt wurden.

**Erläuterung:**

Verweis oder Erläuterung der Regelung zur Löschung oder Vernichtung von personenbezogenen Daten.

1. **Ergänzungen**

Hier können ggf. Ergänzungen eingetragen werden.

**Passwortrichtlinie**

1. Das Passwort besteht aus mindestens 12 oder mehr Zeichen. Je wichtiger das Passwort ist, desto länger sollte es sein. Dies gilt insbesondere bei administrativen Benutzerkonten oder Passwörtern für verschlüsselte Datenträger, Container oder Dateien. Nur in begründeten Ausnahmefällen kann die Anforderung der Passwortlänge unter der Mindestanforderung sein.
2. Das Passwort sollte sowohl Klein- als auch Großbuchstaben, Ziffern und Satzzeichen enthalten.
3. Das Passwort ist nicht im Klartext gespeichert. In begründeten Ausnahmefällen kann das Passwort auch reversibel verschlüsselt gespeichert werden.
4. Zur irreversiblen Speicherung des Passwortes wird ein kryptografisch starker Hash-Algorithmus nach dem Stand der Technik verwendet. Dabei wird auf die Erhöhung der Entropie entweder durch ein kryptografisches „Salt“ und optional einem „Pepper“ oder einem „rehashen“ oder durch eine qualitativ äquivalente Methode bei der Speicherung geachtet.
5. Zur reversiblen Speicherung des Passwortes in begründeten Ausnahmefällen wird ein kryptografisch starkes Verfahren nach dem Stand der Technik verwendet. Die Verwaltung des Passwortes für die Entschlüsselung ist zu erläutern.
6. Das Passwort wird durch den jeweiligen Benutzer eigenständig gewählt und eingegeben.
7. Initiale Passwörter müssen bei der ersten Verwendung geändert werden.
8. Für unterschiedliche Zugänge müssen unterschiedliche Passwörter verwendet werden. Hierfür wird empfohlen die Passwörter mittels eines persönlichen Passwort-Safes zu verwalten.
9. Das Passwort darf nicht leicht zu erraten sein. Insbesondere dürfen nicht verwendet werden
	1. triviale Zeichenfolgen wie „1234“, „qwertz“, „asdf“, usw.,
	2. Wörter, Begriffe oder Namen aus dem privaten oder beruflichen Umfeld oder auch Teile hiervon,
	3. Daten, die man sich als Außenstehender leicht erschließen kann, wie Geburtsdatum, Ort, Straße, usw. zu denen die Person einen Bezug hat.
10. Das Passwort muss bei Verdacht einer Kompromittierung geändert werden. Für den Verdacht reicht es aus, dass das betreffende Konto nur mittelbar durch die Kompromittierung betroffen sein kann.
11. Sofern möglich oder erforderlich sollte eine Zwei-Faktor-Authentifizierung verwendet werden. Hierfür eignet sich zum Beispiel TOTP (Time-based One-time Password Algorithms, RFC 6238). Dies bietet eine erhöhte Sicherheit für die Zugangskontrolle. Der zweite Faktor allein ist **keine** ausreichende Authentifizierung, da dieser nur über Besitz funktioniert.
1. Live-Support ist die direkte Unterstützung des Verantwortlichen durch den Auftragsverarbeiter am Bildschirm des Verantwortlichen. Hierzu kann sich der Auftragsverarbeiter mittels einer Software zur Fernwartung auf den Arbeitsplatzrechner des Verantwortlichen aufschalten und wird dadurch befähigt, Eingaben zu tätigen und Inhalte einzusehen. Kennzeichnend ist, dass ein Mitarbeiter des Verantwortlichen vor dem Bildschirm sitzt und verfolgt, was der Auftragsverarbeiter durchführt. [↑](#footnote-ref-1)
2. Fernwartungsarbeiten sind die Tätigkeiten des Auftragsverarbeiters, die dieser im Rahmen seines Dienstleistungsvertrags (Fehlerbehebung, Aktualisierung o.ä.) entweder durch den Verantwortlichen initiiert (z.B. in einem Ticket-System) oder selbsttätig bearbeitet. Dabei ist ein Mitwirken des Verantwortlichen nicht unmittelbar erforderlich. [↑](#footnote-ref-2)
3. So der Landesbeauftrage für den Datenschutz Baden-Württemberg unter Punkt 4.2 „Maßnahmen zur Zugriffskontrolle“ in der „Checkliste zur Fernwartung“ (Stand 11. Dezember 1998): http://www.baden-wuerttemberg.datenschutz.de/fernwartung/ [↑](#footnote-ref-3)
4. Dies kann insbesondere dann erforderlich sein, wenn der Auftragsverarbeiter eine Client-Umgebung benötigt, die so konfiguriert ist wie die übrigen Clients und eventuell noch zusätzliche Software zur Fehleranalyse usw. benötigt, die man nicht auf dem Server oder einem anderen allgemeinen Client installiert haben möchte. Es kann aber auch dann erforderlich sein, wenn man die Zugangssoftware zur Fernwartung nicht auf dem Server installieren möchte, was vorzuziehen ist, und den Umweg über einen speziellen Arbeitsplatzrechner für die Fernwartung nimmt. [↑](#footnote-ref-4)
5. Art. 28 DS-GVO [↑](#footnote-ref-5)